ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS DIREKTORIUS

ĮSAKYMAS
DĖL ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2020 m. d. Nr.
Šakiai

Vadovaudamasis Lietuvos Respublikos vietos savivaldos įstatymo 18 straipsnio 1 dalimi, 29 straipsnio 8 dalies 2 punktu, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, saugos dokumentų turinio gairių aprašo ir elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7, 8 punktais:

1. T v i r t i n u Šakių rajono savivaldybės administracijos informacinių sistemų naudotojų duomenų saugos nuostatus (pridedama);

3. P r i p a ž į s t u netekusiu galios Šakių rajono savivaldybės administracijos direktoriaus 2018 m. lapkričio 12 d. įsakymą Nr. AT-1069 „Dėl Šakių rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatų patvirtinimo“.

Šis įsakymas per vieną mėnesį nuo įsakymo paskelbimo dienos gali būti skundžiamas Lietuvos administracinių ginčų komisijos Kauno apygardos skyriui adresu: Laisvės al. 36, Kaunas, arba Regionų apygardos administracinio teismo Kauno rūmams adresu: A. Mickevičiaus g. 8A, Kaunas.

Administracijos direktorius Dainius Grincevičius

Parengė
Bendrųjų reikalų skyriaus vedėja

Rita Vaičiūnienė
2020-07-30

SUDERINTA
Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos
2020-08-13 raštu Nr. (4.1 E) 6K-515

PATVIRTINTA
Šakių rajono savivaldybės
administracijos direktoriaus
2020 m. d.
įsakymu Nr. AT-

ŠAKIŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

Šakių rajono savivaldybės administracijos (toliau − Savivaldybės administracija) informacinių sistemų (toliau – IS) duomenų saugos nuostatai (toliau – saugos nuostatai) nustato sistemose tvarkomos elektroninės informacijos saugos tikslus, elektroninės informacijos saugos užtikrinimo prioritetines kryptis, saugų elektroninės informacijos valdymą, organizacinius, techninius ir personalui keliamus reikalavimus, naudotojų supažindinimo su saugos dokumentais principus, apibrėžia elektroninės informacijos saugos politiką.

2. Saugos nuostatuose vartojamos sąvokos:

Administratorius – savivaldybės administracijos valstybės tarnautojas ar darbuotojas, dirbantis pagal sutartį, užtikrinantis IS veikimą ir saugą.

Elektroninės informacijos saugos incidentas – įvykis ar veiksmas, kuris gali sudaryti neteisėto prisijungimo prie informacinės sistemos galimybę, sutrikdyti ar pakeisti informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai pasisavinti elektroninę informaciją ją paskleisti ar kitaip panaudoti.

Informacinės sistemos naudotojas – valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, turintis teisę naudotis informacinės sistemos ištekliais numatytoms funkcijoms atlikti.

Informacinės sistemos saugos įgaliotinis – savivaldybės administracijos direktoriaus paskirtas valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, koordinuojantis ir prižiūrintis saugos politikos įgyvendinimą.

Kitos saugos nuostatuose vartojamos sąvokos atitinka sąvokas nustatytas Lietuvos Respublikos įstatymuose ir kituose teisės aktuose bei Lietuvos standartais LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014.

3. IS saugos nuostatų tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją Šakių rajono savivaldybės administracijos informacinėse sistemose.

4. Saugos nuostatai, saugaus elektroninės informacijos tvarkymo taisyklės, veiklos tęstinumo valdymo planas, naudotojų administravimo taisyklės (toliau visi kartu – IS saugos dokumentai) privalomi:

4.1. IS valdytojui – Šakių rajono savivaldybės administracijai, Bažnyčios g. 4, Šakiai;

4.2. IS tvarkytojui – Šakių rajono savivaldybės administracijai, Savivaldybės biudžetinėms įstaigoms;

4.3. IS saugos įgaliotiniui;

4.4. IS administratoriams;

4.5. IS naudotojams – IS valdytojo valstybės tarnautojams ar darbuotojams, dirbantiems pagal darbo sutartį, arba IS tvarkytojo darbuotojams, pagal kompetenciją naudojantiems ir (ar) tvarkantiems elektroninę informaciją.

5. Savivaldybės administracijos direktoriaus tvirtinamos saugaus elektroninės informacijos tvarkymo taisyklės, IS veiklos tęstinumo valdymo planas ir IS naudotojų administravimo taisyklės yra duomenų saugos nuostatuose nustatytą duomenų saugos politiką įgyvendinantys teisės aktai.

6. IS saugos nuostatai parengti vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų bei Saugos dokumentų turinio gairių aprašais, patvirtintais Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ ir kitais teisės aktais, reglamentuojančiais duomenų tvarkymo teisėtumą.

7. IS elektroninės informacijos saugumas užtikrinamas, vadovaujantis šiomis prioritetinėmis kryptimis:

7.1. įgyvendinant atliekamų veiksmų su IS elektronine informacija automatinį stebėjimą ir įrašų kaupimą;

7.2. suteikiant naudotojams prieigos teises prie IS elektroninės informacijos ir identifikuojant IS naudotojų tapatumą;

7.3. kopijuojant IS duomenų bazę, saugant archyve esančias kopijas;

7.4. saugant IS elektroninę informaciją nuo žalingos programinės įrangos poveikio;

7.5. įrengiant saugias informacinei sistemai tvarkyti skirtas patalpas ir kompiuterizuotas darbo vietas jose;

7.6. tobulinant IS naudotojų kvalifikaciją;

7.7. įgyvendinant IS elektroninės informacijos integralumą su registrais ir informacinėmis sistemomis;

7.8. įgyvendinant IS elektroninės informacijos saugos priemones nuo nesankcionuoto poveikio IS programinei, techninei įrangai ir (ar) IS programinės įrangos modifikavimo;

7.9. įgyvendinant IS veiklos tęstinumą.

8. Šakių rajono savivaldybės administracija, kaip IS valdytojas:

8.1. pagal kompetenciją atsako už saugos politikos formavimą, jos įgyvendinimo organizavimą ir priežiūrą;

8.2. tvirtina IS saugos dokumentus ir kitus teisės aktus, kuriuose reglamentuojamas IS tvarkymo teisėtumas ir IS elektroninės informacijos sauga;

8.3. analizuoja IS saugos įgaliotinio pateiktus siūlymus, priima sprendimus dėl IS techninių ir programinių priemonių, būtinų IS elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

8.4. skiria IS saugos įgaliotinį, paveda jam organizuoti IS saugos politiką ir kontroliuoti jos įgyvendinimą;

8.5. atlieka kitas IS Saugos nuostatų ir IS saugos dokumentuose jam nustatytas funkcijas.

9. IS tvarkytojų vadovų (skyrių ir tarnybų vedėjų, seniūnų) funkcijos ir atsakomybė:

9.1. rūpinasi IS saugumu, vykdo IS valdytojo nurodymus;

9.2. atsako už IS saugos reikalavimų atitiktį galiojantiems teisės aktams ir šiems Informacinių sistemų saugos nuostatams;

9.3. užtikrina, kad IS tvarkytojo darbuotojai – Savivaldybės administracijos valstybės tarnautojai ar darbuotojai, dirbantys pagal darbo sutartį, kurie tvarko ar naudojasi IS ištekliais numatytoms funkcijoms atlikti, laikytųsi nuostatų, išvardintų saugos nuostatuose ir saugos politiką įgyvendinančiuose teisės aktuose;

10. IS saugos įgaliotinio funkcijos ir atsakomybė:

10.1. teikia IS valdytojo vadovui pasiūlymus dėl IS saugos dokumentų priėmimo, keitimo ar panaikinimo;

10.2. koordinuoja elektroninės informacijos saugos incidentų tyrimą;

10.3. pasirašytinai supažindina IS tvarkytojų darbuotojus su saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais bei atsakomybe už šių reikalavimų nesilaikymą;

10.4. organizuoja IS tvarkytojų darbuotojų kvalifikacijos tobulinimą duomenų saugos klausimais, reguliariai jiems primena saugumo problemas;

10.5. organizuoja IS rizikos vertinimą;

10.6. atlieka kitas IS valdytojo vadovo jam priskirtas funkcijas informacinių sistemų saugos klausimais;

10.7. atsako už IS saugos politikos įgyvendinimo organizavimą bei IS saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams.

11. IS administratoriaus funkcijos ir atsakomybė:

11.1. atsako už IS funkcionavimą;

11.2. įvertina IS naudotojų pasirengimą dirbti su informacine sistema ir suteikia jiems teisę naudotis informacinės sistemos galimybėmis priskirtoms funkcijoms atlikti;

11.3. rengia pasiūlymus IS kūrimo, palaikymo, priežiūros ir duomenų saugos klausimais;

11.4. atlieka IS sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, duomenų perdavimo tinklų) administravimą, pažeidžiamų vietų ir saugos reikalavimų atitikties nustatymą;

11.5. registruoja ir informuoja IS saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia pasiūlymus.

12. Duomenų sauga IS užtikrinama vadovaujantis:

12.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

12. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

12.3. Lietuvos Respublikos kibernetinio saugumo įstatymu;

12.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“.

12.5. Lietuvos standartais LST ISO/IEC 27001 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“.

12.6. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 10 punktu, Sistemose tvarkoma informacija priskiriama mažiausios svarbos informacijos kategorijai.

14. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 12.4 papunkčiu, IS priskiriamas ketvirtajai informacinių sistemų kategorijai.

15. IS saugos įgaliotinis:

15.1. atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja IS rizikos įvertinimą. Pasikeitus IS duomenų bazės struktūrai (sistemos pakeitimai, papildymas naujomis taikomosiomis programomis, taikomųjų programų šalinimas ir kt.) ar nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis IS rizikos įvertinimas;

15.2. IS rizikos įvertinimą išdėsto įvertinimo ataskaitoje. IS įvertinimo ataskaita rengiama, atsižvelgus į rizikos veiksnius, galinčius turėti ar turinčius įtakos IS elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę, galimus rizikos valdymo būdus. Svarbiausieji rizikos veiksniai yra šie:

15.2.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kita);

15.2.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis elektronine informacija, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

15.2.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte;

15.3. Rizikos įvertinimo ataskaita pateikiama IS valdytojui.

16. IS valdytojo vadovui patvirtinus IS rizikos įvertinimo ataskaitą, prireikus rengiamas IS rizikos įvertinimo ir rizikos valdymo priemonių planas, kuriame numatomos techninės ir administracinės veiksnius šalinančios priemonės, priemonių vykdymo terminai, vykdytojai ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti. IS rizikos įvertinimo ir rizikos valdymo priemonių planą tvirtina IS valdytojas.

17. IS elektroninei informacijai, techninei, programinei įrangai, patalpoms IS valdytojo įstaigoje vertinti naudojama penkiabalė rizikos veiksnių tikėtumo ir žalos vertinimo metodika:

17.1. nereikšminga rizikos veiksnių tikimybė, žala – 1 balas;

17.2. maža rizikos veiksnių tikimybė, žala – 2 balai;

17.3. vidutinė rizikos veiksnių tikimybė, žala – 3 balai;

17.4. didelė rizikos veiksnių tikimybė, žala – 4 balai;

17.5. labai didelė rizikos veiksnių tikimybė, žala – 5 balai.

18. IS saugos priemonės parenkamos, įvertinus galimus rizikos veiksnius IS elektroninės informacijos vientisumui ir prieinamumui.

19. IS elektroninės informacijos saugos priemonių parinkimo pagrindiniai principai yra tokie:

19.1. saugos priemonės turi būti valdomos centralizuotai;

19.2. saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei;

19.3. likutinė rizika turi būti sumažinta iki priimtino lygio;

19.4. kur galima, būtina įdiegti prevencines informacijos saugos priemones;

19.5. IS veiklos tęstinumo ir elektroninės informacijos sauga turi būti užtikrinama, patiriant kuo mažiau išlaidų.

20. Siekiant įvertinti IS saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per dvejus metus organizuojamas IS informacinių technologijų saugos atitikties vertinimas:

20.1. IS saugos atitikties vertinimą organizuoja saugos įgaliotinis;

20.2. įvertinama IS saugos dokumentų ir realios informacijos saugos situacijos atitiktis;

20.3. inventorizuojama IS techninė ir programinė įranga;

20.4. patikrinama (įvertinama) IS naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis IS saugos dokumentams;

20.5. įvertinamas pasirengimas užtikrinti IS veiklos tęstinumą, įvykus saugos incidentui.

21. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama IS informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama IS valdytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus skiria ir įgyvendinimo terminus nustato IS valdytojo vadovas.

Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijos, informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijos ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikiamos Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

22. Programinės įrangos, skirtos IS nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai) apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

22.1. IS tarnybinių stočių ir kompiuterinėse darbo vietose turi būti kenksmingos programinės įrangos aptikimo priemonės, kurioms turi būti reguliariai tikrinami atnaujinimai automatiniu būdu ne rečiau kaip kartą per parą;

22.2. turi būti naudojamos priemonės, nuolat ieškančios ir blokuojančios kenksmingą programinę įrangą, veikiančią sisteminiuose kataloguose esančiose tarnybinės stoties rinkmenose ir visuose kompiuterių tinklo kompiuteriuose;

22.3. turi būti naudojamos priemonės, turinčios apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų.

23. Programinės įrangos, įdiegtos kompiuteriuose ir tarnybinėse stotyse, naudojimo nuostatos:

23.1. turi būti naudojama tik legali, programinė įranga;

23.2. programinė įranga turi būti nuolat atnaujinama, laikantis gamintojo reikalavimų;

23.3. programinę įrangą diegti, šalinti ir konfigūruoti gali tik IS sisteminės priežiūros ir tvarkymo administratorius;

23.4. turi būti įdiegta prieigos prie IS elektroninės informacijos per registravimąsi, teisių suteikimą ir slaptažodžius sistema;

23.5. turi būti įgyvendinta prievolė ne rečiau kaip kas tris mėnesius keisti slaptažodžius;

23.6. turi būti įdiegta galimybė fiksuoti ir kaupti informaciją apie asmenų, kurie naudojosi prieiga prie IS elektroninės informacijos, atliktus veiksmus.

24. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kita) pagrindinės naudojimo nuostatos:

24.1. IS elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų, naudojant ugniasienes, ugniasienių įvykių žurnalai turi būti reguliariai analizuojami;

24.2. IS programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atjungimo, atskyrimo nuo paslaugos (angl. *DOS*), dedikuoto atjungimo, atskyrimo nuo paslaugos (angl. *DDOS*);

24.3. informacinės sistemos tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių IS naudotojų kompiuterinę įrangą nuo kenksmingo kodo.

25. Leistinos kompiuterių naudojimo ribos:

25.1. stacionarūs ir nešiojamieji IS naudotojų kompiuteriai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi IS duomenys ir IS informacija;

25.2. kompiuteriuose turi būti naudojamas įjungimo slaptažodis;

25.3. IS naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo;

25.4. IS valdytojo stacionarų kompiuterį prijungti prie IS kompiuterių tinklo gali tik IS sisteminės priežiūros ir tvarkymo administratorius;

25.5. išvežti iš patalpų nešiojamieji kompiuteriai negali būti palikti be priežiūros viešose vietose; kelionės metu nešiojamieji kompiuteriai turi būti saugomi;

25.6. visų nešiojamų kompiuterių failų sistema turi būti šifruojama AES 128 arba AES 256 šifravimo sistema.

26. Metodai, kuriais užtikrinamas saugus IS elektroninės informacijos teikimas ir (ar) gavimas:

26.1. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą iš kitų valstybės institucijų, naudojami saugūs ryšio kanalai, kuriais perduodami šifruoti duomenys;

26.2. elektroninė informacija iš susijusių registrų gaunama tik pagal duomenų teikimo ir gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką;

26.3. prieigos prie IS elektroninės informacijos teises gali suteikti tik IS sisteminės priežiūros ir tvarkymo administratorius. IS naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės;

26.4. prieiga prie IS elektroninės informacijos leidžiama tik per registravimosi slaptažodžių sistemą. Prieigos prie IS elektroninės informacijos valdymas apibrėžtas IS naudotojų administravimo taisyklėse;

26.5. pasibaigus IS naudotojo darbo sutarčiai, teisė naudotis IS elektronine informacija turi būti panaikinta. IS naudotojui prieiga prie IS turi būti ribojama ar sustabdoma, kai vyksta IS naudotojo veiklos tyrimas, naudotojas turi ilgalaikes atostogas arba keičiasi jo atliekamos ir (ar) pareigybės aprašyme nurodytos funkcijos.

27. IS atsarginės duomenų bazės kopijos daromos automatiniu būdu kiekvieną dieną, esant aktyviai IS duomenų bazei. Kopijos, arba laikmena, kuriose laikomos kopijos privalo būti šifruojamos AES ar XTS-AES, nemažiau kaip 128 bitų ilgio raktu. Prireikus jas atkurti turi teisę tik sisteminės priežiūros ir tvarkymo administratorius ar jį pavaduojantis asmuo. Kopijų darymo ir saugojimo tvarka nustatoma IS saugaus elektroninės informacijos tvarkymo taisyklėse.

IV. REIKALAVIMAI PERSONALUI

28. IS saugos įgaliotinis privalo išmanyti pagrindinius informacijos saugos principus.

29. IS administratorius turi išmanyti informacijos saugos principus, darbą su kompiuterių tinklais, mokėti užtikrinti jų saugumą, taip pat administruoti ir prižiūrėti duomenų bazes, turi būti susipažinęs su saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais, taip pat kitomis vidaus ir darbo saugos taisyklėmis.

30. IS tvarkytojų darbuotojai privalo turėti pagrindinių darbo su kompiuteriu įgūdžių, mokėti tvarkyti IS duomenis ir būti susipažinę su saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais.

31. IS naudotojai privalo turėti pagrindinių darbo su kompiuteriu įgūdžių, būti susipažinę su saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais.

32. IS tvarkytojai ir IS naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veiklos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti IS saugos įgaliotiniui ir / arba IS administratoriui.

33. Teisės, personalo ir civilinės metrikacijos skyrius organizuoja naudotojų mokymus duomenų saugumo klausimais.

V. INFORMACINIŲ SISTEMŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

34. IS duomenis gali naudoti tik tie asmenys, kurie susipažinę su saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais ir raštiškai sutikę laikytis šių teisės aktų reikalavimų.

35. Už IS naudotojų supažindinimą su saugos nuostatais ir dokumentais, įgyvendinančiais saugos politiką, atsako IS saugos įgaliotinis.

36. IS naudotojai, pažeidę saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

VI. BAIGIAMOSIOS NUOSTATOS

37. IS saugos dokumentai gali būti keičiami. Saugos dokumentų pakeitimai turi būti derinami ir tvirtinami teisės aktų nustatyta tvarka.

38. IS saugos įgaliotinis saugos dokumentus turi persvarstyti (peržiūrėti) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos įvertinimą ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems IS valdytojo veiklos pokyčiams. Saugos dokumentų peržiūros rezultatai įrašomi į rizikos vertinimo ataskaitą.

39. IS naudotojai, administratoriai, saugos įgaliotinis, pažeidę IS duomenų saugos politiką įgyvendinančių dokumentų reikalavimus, atsako teisės aktų nustatyta tvarka.

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Šakių rajono savivaldybė
Dokumento pavadinimas (antraštė)	Dėl Šakių rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatų patvirtinimo
Dokumento registracijos data ir numeris	2020-08-20 13:17 Nr. AT-698
Dokumento gavimo data ir dokumento gavimo registracijos numeris	-
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Dainius Grincevičius Administracijos direktorius
Parašo sukūrimo data ir laikas	2020-08-20 13:17
Parašo formatas	Trumpalaikio galiojimo (XAdES-T)
Laiko žymoje nurodytas laikas	2020-08-20 13:17
Informacija apie sertifikavimo paslaugų teikėją	ADIC CA-A
Sertifikato galiojimo laikas	2018-02-05 10:41 - 2021-02-04 10:41
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	0
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	informaciniu sistemu_duomenu saugos nuostatai.docx
Pridedamo dokumento registracijos data ir numeris	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	DekaDoc v.20200814.3
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2020-08-20 15:20 nuorašą suformavo Irena Bacevičienė
Paieškos nuoroda	-
Papildomi metaduomenys	-